

## AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application:

### Listing of claims:

- 1                    1. (Currently Amended)        An advanced encryption standard (AES) engine  
2                    with real time S-box generation comprising:  
3                                    a Galois field multiplier system in a first mode responsive to a first data  
4                    block for generating an AES selection (S-box) function by executing the multiplicative  
5                    inverse increase in  $[[GF^1]] \underline{GF^{-1}} (2^m)$  and applying an affine over GF(2) transformation to  
6                    obtain a subbyte transformation; and  
7                                    a shift register system for transforming said subbyte transformation to  
8                    obtain a shift row transformation;  
9                                    said Galois field multiplier system being responsive in a second mode to  
10                    said shift row transformation to obtain a mix column transformation and adding a round  
11                    key for generating in real time an advanced encryption standard cipher function of said  
12                    first data block.
- 1                    2. (Previously presented) The advanced encryption standard (AES) engine with  
2                    real time S-box generation of claim 1 in which said first mode includes two states for  
3                    executing m-1 cycles of operation including a first state for multiplying a subbyte by one  
4                    to obtain a product and then squaring the product to obtain an intermediate result and  
5                    repeating with the intermediate result m-2 times and a second state for performing the  
6                    multiply and square operations one more time and transforming the final intermediate

7 result to obtain the subbyte transformation.

1 3. (Original) The advanced encryption standard (AES) engine with real time S-  
2 box generation of claim 2 in which said Galois field multiplier system includes a Galois  
3 field linear transformer for each said mode.

1 4. (Original) The advanced encryption standard (AES) engine with real time S-  
2 box generation of claim 2 in which said Galois field multiplier system includes a Galois  
3 field linear transformer for each state of said first mode and for said second mode.

1 5. (Original) The advanced encryption standard (AES) engine with real time S-  
2 box generation of claim 2 in which said Galois field multiplier system includes a Galois  
3 field linear transformer and a program circuit for reconfiguring said Galois field linear  
4 transformer for each mode.

1 6. (Original) The advanced encryption standard (AES) engine with real time S-  
2 box generation of claim 5 in which said program circuit further reconfigures said Galois  
3 field linear transformer for each state in said first mode.

1 7. (Original) The advanced encryption standard (AES) engine with real time S-  
2 box generation of claim 5 in which said program circuit configures said Galois field  
3 linear transformer to perform a compound multiply-square operation in said first state.

1           8. (Original) The advanced encryption standard (AES) engine with real time S-  
2 box generation of claim 5 in which said program circuit configures said Galois field  
3 linear transformer to perform a compound multiply-square operation in said first state and  
4 a compound multiply-square and affine subbyte transformation in said second state.

1           9. (Original) The advanced encryption standard (AES) engine with real time S-  
2 box generation of claim 3 in which said Galois field linear transformer associated with  
3 said second mode is configured as a multiplier in said first state and as multiply-  
4 accumulate in said second state to perform a mix column transformation and add a round  
5 key for generating an advanced encryption standard cipher function of said first data  
6 block.

1           10. (Original) The advanced encryption standard (AES) engine with real time S-  
2 box generation of claim 3 in which said Galois field linear transformer associated with  
3 said first state is configured as a multiplier to perform a compound multiply-square  
4 operation.

1           11. (Original) The advanced encryption standard (AES) engine with real time S-  
2 box generation of claim 3 in which said Galois field linear transformer associated with  
3 said second state is configured as a multiply-adder to perform a compound multiply-  
4 square and affine subbyte transformation.

1           12. (Original) The advanced encryption standard (AES) engine with real time S-

2 box generation of claim 1 in which said Galois field multiplier system includes at least  
3 one Galois field linear transformer and an associated polynomial multiplier.

1 13. (Original) The advanced encryption standard (AES) engine with real time S-  
2 box generation of claim 1 in which said Galois field multiplier system includes a  
3 reconfigurable matrix of cells.

1 14. (Original) The advanced encryption standard (AES) engine with real time S-  
2 box generation of claim 1 further including a key generator for providing a plurality of  
3 round keys.

1 15. (Original) The advanced encryption standard (AES) engine with real time S-  
2 box generation of claim 14 in which said key generator includes a key generator circuit  
3 responsive to a master key to generate said round keys.

1 16. (Original) The advanced encryption standard (AES) engine with real time S-  
2 box generation of claim 15 in which said key generator circuit includes said Galois field  
3 multiplier system in a third mode for executing a multiplicative inverse in  $GF^1(2^m)$  and  
4 applying affine over  $GF(2)$  transformation to obtain said round keys.

1 17. (Original) The advanced encryption standard (AES) engine with real time S-  
2 box generation of claim 16 in which said round key includes a plurality of subkeys.

1           18. (Previously presented) The advanced encryption standard (AES) engine with  
2           real time S-box generation of claim 17 in which said third mode includes two states for  
3           executing m-1 cycles of operation including a third state for multiplying a subkey by one  
4           to obtain a product and then squaring the product to obtain an intermediate result and  
5           repeating with the intermediate result m-2 times and a fourth state for performing the  
6           multiply and square operations one more time and transforming the final infinite result to  
7           obtain the subkey transformation.

1           19. (Original) The advanced encryption standard (AES) engine with real time S-  
2           box generation of claim 18 in which said Galois field multiplier system includes a Galois  
3           field transformer for each of said third and fourth states.

1           20. (Original) The advanced encryption standard (AES) engine with real time S-  
2           box generation of claim 19 in which said Galois field linear transformer is reconfigured  
3           by said program circuit for said third mode.

1           21. (Original) The advanced encryption standard (AES) engine with real time S-  
2           box generation of claim 20 in which said program circuit for further reconfigures said  
3           Galois field linear transformer for each of said third and fourth states in said third mode.

1           22. (Original) The advanced encryption standard (AES) engine with real time S-  
2           box generation of claim 20 in which said program circuit configures said Galois field  
3           linear transformer to perform a compound multiply-square operation in said third state.

1           23. (Original) The advanced encryption standard (AES) engine with real time S-  
2 box generation of claim 20 in which said program circuit configures said Galois field  
3 linear transformer to perform a compound multiply-square operation and affine subkey  
4 transformation in said fourth state.

1           24. (Original) The advanced encryption standard (AES) engine with real time S-  
2 box generation of claim 18 in which said Galois field linear transformer associated with  
3 said third state mode is configured as a multiplier to perform a compound multiply-  
4 square operation.

1           25. (Original) The advanced encryption standard (AES) engine with real time S-  
2 box generation of claim 18 in which said Galois field linear transformer associated with  
3 said fourth state is configured as a multiply-adder to perform a compound multiply-  
4 square and affine subkey transformation.

1           26. (Original) The advanced encryption standard (AES) engine with real time S-  
2 box generation of claim 1 in which said Galois field multiplier system includes: a  
3 polynomial multiplier circuit for multiplying two polynomials with coefficients over a  
4 Galois field to obtain their product; a Galois field linear transformer responsive to said  
5 polynomial multiplier circuit for predicting the modulo remainder of the polynomial product  
6 for an irreducible polynomial; a storage circuit for supplying to said Galois field linear  
7 transformer a set of coefficients for predicting the modulo remainder for a predetermined  
8 irreducible polynomial; and a Galois field adder circuit for adding said product of said

multiplier circuit with a third polynomial with coefficients over a Galois field for performing the compound multiply and add operations in a single cycle.

27. (Original) The advanced encryption standard (AES) engine with real time S-box generation of claim 1 in which said Galois field multiplier system includes: a polynomial multiplier circuit for multiplying two polynomials with coefficients over a Galois field to obtain their product; a Galois field linear transformer responsive to said polynomial multiplier circuit for predicting the modulo remainder of the polynomial product for an irreducible polynomial; a storage circuit for supplying to said Galois field linear transformer a set of coefficients for predicting the modulo remainder for a predetermined irreducible polynomial; and a Galois field adder circuit for adding said product of said multiplier circuit with an additive identity polynomial for performing a Galois field multiply function of the input polynomials in one cycle.

28. (Original) The advanced encryption standard (AES) engine with real time S-box generation of claim 1 in which said Galois field multiplier system includes: a polynomial multiplier circuit for multiplying two polynomials with coefficients over a Galois field to obtain their product; a Galois field linear transformer responsive to said polynomial multiplier circuit for predicting the modulo remainder of the polynomial product for an irreducible polynomial; a storage circuit for supplying to said Galois field linear transformer a set of coefficients for predicting the modulo remainder for a predetermined irreducible polynomial; and a Galois field adder circuit for adding said product of said multiplier circuit with said output of said Galois field linear transformer circuit to obtain

10       Galois field multiply-accumulate function of the input polynomials in one cycle.

1           29. (Original) The advanced encryption standard (AES) engine with real time S-  
2       box generation of claim 1 further including a plurality of Galois field multiplier systems  
3       for simultaneously processing a plurality of subbytes.

1           30. (Original) The advanced encryption standard (AES) engine with real time S-  
2       box generation of claim 17 further including a plurality of Galois field multiplier systems  
3       for simultaneously processing a plurality of subkeys.

1           31. (Original) The advanced encryption standard (AES) engine with real time S-  
2       box generation of claim 3 in which said Galois field linear transformer has a matrix of  
3       cells for immediately predicting the modulo remainder of the succession of Galois field  
4       linear transforms of an irreducible Galois field polynomial to obtain the ultimate output  
5       of the Galois field linear transform directly in one transform cycle.